

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of Rules and Regulations
Implementing the Telephone Consumer
Protection Act of 1991

CG Docket No. 02-278

Assurance IQ, LLC's Petition for Expedited
Declaratory Ruling Regarding the Application
of 47 U.S.C. § 227(b)(1) of the Telephone
Consumer Protection Act

**Comments of James Shelton in Opposition to Petition for Expedited Declaratory Ruling
filed by Assurance IQ, LLC**

Anthony I. Paronich
Paronich Law, P.C.
350 Lincoln Street, Ste. 2400
Hingham, MA 02043
(508) 221-1510

Keith J. Keogh
Timothy J. Sostrin
KEOGH LAW LTD
55 W Monroe St, Ste 3390
Chicago, IL 60603
(312) 726-1092

June 22, 2020

Attorneys for James Shelton

Table of Contents

| | |
|---|-----------|
| I. LEAD GENERATION FRAUD – AN INTRODUCTION | 1 |
| II. THE COMMISSION SHOULD NOT RE-DEFINE “PRIOR EXPRESS CONSENT” | 3 |
| A. The Plain Language of the TCPA Precludes Adoption of the Proposed “Reasonable Basis to Believe” Rule..... | 4 |
| B. The Commission has Repeatedly Declined to Adopt Similar Broadly Sweeping Rules | 6 |
| C. A “Reasonable Basis to Believe” Rule Would Harm Consumers and Create Confusion | 8 |
| 1. Fraud is Rampant in the Telemarketing Lead Generation Industry | 9 |
| 2. Website’s Like Assurance’s Incentive Lead Generation Fraud..... | 11 |
| III. THE COMMISSION SHOULD NOT CREATE A SAFE HARBOR FOR “CONSENT DATA” | 16 |
| IV. THE COMMISSION CANNOT AND SHOULD NOT EXEMPT “SHORT, INTRODUCTORY PRERECORDED MESSAGES” FROM THE TCPA | 18 |
| V. A RESPONSE TO THE AD HOMINEM ATTACK ON MR. SHELTON | 23 |

I. LEAD GENERATION FRAUD – AN INTRODUCTION

The personally identifying information of millions of Americans is trafficked over the internet every day. Consumers’ names, telephone numbers, email addresses, and phone numbers are bought, sold, and sometimes stolen, by hundreds of data brokers, bots, and other entities that these consumers will never personally interact with and will probably never even hear about.¹

Assurance is both a data broker² and a telemarketer. It claims that James Shelton’s name, phone number, and email address were uploaded to its website on a page that contains a TCPA consent disclosure, however it does not contend that Mr. Shelton himself uploaded the information. Instead, it acknowledges that this is a “fraudulent internet lead scenario”³ and that Mr. Shelton’s personal data was uploaded by a TOR Exit Router⁴ – a favorite tool of internet fraudsters, given that it disguises the IP address of the party accessing the site.⁵

One need look no further than the consent disclosure on Assurance’s website to see why this fraud occurred. The disclosure doesn’t simply authorize Assurance to sell consumer data or place phone calls; it authorizes literally hundreds of distinct entities, from jewelers, to insurance companies, to debt relief companies, to solar panel suppliers, to place telemarketing calls to whatever phone numbers are uploaded on the site. Every single one of those entities, along with

¹ DATA BROKERS ARE SELLING YOUR SECRETS. HOW STATES ARE TRYING TO STOP THEM., (June 24, 2019), available at <https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-your-secrets-how-states-are-trying-stop-them/>

² Assurance registered as a data broker with the State of Vermont on March 6, 2019. <https://bizfilings.vermont.gov/online/DatabrokerInquire/>

³ Petition, at p. 9.

⁴ Petition, at p. ii.

⁵ TOR AND WHY FRAUDSTERS EXPLOIT IT, <https://www.idology.com/blog/tor-and-why-fraudsters-exploit-it/>.

any lead generation business, data broker, or affiliate marketer that they may hire, has a financial incentive to upload consumer data to the website because they can then use the data in telemarketing calls, earn commissions for generating the leads, or sell it to others who wish to do so.

Given these incentives, lead generation fraud is becoming a major problem for both consumers and businesses alike, and particularly in the context of “affiliate marketing.” “Affiliates,” seeking to earn a commission by generating leads for telemarketers to call, often fill out lead generation forms with stolen or fraudulent consumer information. The fraudsters simply copy the consumer data into the forms, thus “generating” leads for the affiliate company and boosting their commissions.⁶ And fraudsters don’t need to upload each lead manually – they often program “bots” to submit the fraudulent information for them⁷ and can even dump entire lists of leads through an API or FTP site set up by the marketer.⁸

Assurance’s petition asks the Commission to rule that Mr. Shelton, and any other consumer whose personal information is fraudulently trafficked on the internet, should bear the burden of this fraud, rather than the robocallers who seek to call them. It specifically proposes that robocallers should be allowed to use prerecorded messages to call phone numbers uploaded on internet consent forms until the called party tells them that, in fact, they do not consent. In the case of Assurance’s website, any consumer whose information was uploaded on that site would

⁶ HOW LEAD GENERATION FRAUD AFFECTS BRANDS AND CONSUMERS, <https://blog.anura.io/how-lead-fraud-affects-brands-and-consumers>;

⁷ FRAUDULENT WEB TRAFFIC CONTINUES TO PLAGUE ADVERTISERS, OTHER BUSINESSES, <https://www.wsj.com/articles/fraudulent-web-traffic-continues-to-plague-advertisers-other-businesses-1522234801>

⁸ HOW LEAD FRAUD HAPPENS, <https://www.databowl.com/blog/posts/2015/10/07/how-lead-fraud-happens.html>

need to tell literally hundreds of distinct entities that they do not consent to be called before they could ever assert their rights under the TCPA against them. The Commission should decline to adopt such a rule for the reasons set forth below.

II. THE COMMISSION SHOULD NOT RE-DEFINE “PRIOR EXPRESS CONSENT”

Assurance seeks a “declaratory ruling regarding the application of 47 U.S.C. § 227(b)(1) of the Telephone Consumer Protection Act.”⁹ § 227(b)(1) requires telemarketers to obtain the “prior express consent of the called party” before placing any robocalls to a cellular telephone number.¹⁰ Assurance asks the Commission to rule that robocallers need not *actually* have prior express consent of the called party, but instead need only “*a reasonable basis to believe* that they have the prior express consent of the called party.”¹¹ It further requests the Commission to rule that where a telemarketer possesses data purporting to show that a consumer gave prior express consent, it should be able robocall that consumer “until such time as the called party claims to the caller that he or she did not provide the consent.”¹²

Neither the plain language of the statute, nor any ruling of any federal court of appeals, give the Commission the authority to re-define “prior express consent” in this way. Moreover, such a rule, even if it were within the scope of the Commission’s authority to adopt, would have terrible implications for consumers who are already overwhelmed with robocalls from

⁹ Petition, at cover.

¹⁰ 47 U.S.C. § 227(b)(1)

¹¹ Petition, at pp. 12-13.

¹² *Ibid.*

telemarketers to the point that they now often avoid answering the phone entirely.¹³

A. The Plain Language of the TCPA Precludes Adoption of the Proposed “Reasonable Basis to Believe” Rule

“When Congress includes particular language in one section of a statute but omits it in another” courts must “presume that Congress intended a difference in meaning.” *Loughrin v. United States*, 573 U.S. 351, 358 (2014). The TCPA is a perfect example.

The TCPA contains myriad provisions governing the conduct of telemarketers. Some of those provisions expressly require consideration of the telemarketer’s knowledge, beliefs, or intent, and others, like the provision at issue here (§ 227(b)(1)), contain no such language.

For instance, the provision regarding caller-id spoofing states that “[i]t shall be unlawful . . . to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value[.]” See 47 U.S.C. § 227(e)(1) (emphasis added). The provision at issue here, on the other hand, makes no reference to the caller’s knowledge or intent and simply provides that “it shall be unlawful . . . to make any call (other than a call made for emergency purposes or made with the prior express consent of the called party) using any automatic telephone dialing system or an artificial or prerecorded voice . . . to any telephone number assigned to a . . . cellular telephone service[.]” 47 U.S.C. § 227(b)(1). Thus, it must be presumed that Congress did not intend for a caller’s knowledge or intent to have any bearing on whether a violation of § 227(b)(1) is committed.

Likewise, Congress drafted the statute to expressly require consideration of the caller’s knowledge and intent in (1) determining the *amount of damages* to award in civil actions brought

¹³ *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, 33 FCC Rcd 12024, 12025-26, ¶ 4 (December 12, 2018) (“2018 Order”) (“We have received hundreds of comments from consumers stating that they no longer answer their phone when it rings.”)

by consumers (*i.e.*, whether violations were committed “willfully or knowingly”);¹⁴ (2) determining the *amount of damages* to award in civil actions brought by *states* (same);¹⁵ and (3) determining whether the commission can impose a *heightened forfeiture penalties* of \$10,000 in its own enforcement actions (*i.e.*, whether the violation was committed “with the intent to cause such violation”).¹⁶ All of these provisions make a telemarketer’s reasonable belief about consent relevant in assessing the amount of damages and/or penalties that can be awarded, but there are no such considerations in determining whether or not a violation occurred in the first place. Indeed, there would be little point in Congress drafting these treble damages provisions if every violation of § 227(b)(1) must already be “objectively unreasonable” in order to create liability in the first place.¹⁷

Given the plain language of the statute, “[t]he circuit courts that have considered whether intent is relevant to TCPA liability have all concluded that good faith error or mistake does not preclude a defendant’s liability but is material only to the question of treble damages for willful conduct.”¹⁸ Thus, “[t]he TCPA is essentially a strict liability statute . . . [and] does not require

¹⁴ See 47 U.S.C. § 227(b)(3) (providing that court may award treble damages in actions brought for violations of § 227(b) “[i]f the court finds that the defendant *willfully or knowingly* violated this subsection or the regulations prescribed under this subsection”); see also, 47 U.S.C. § 227(c)(5) (same provision for actions brought for violation of § 227(c)).

¹⁵ See 47 U.S.C. § 227(g)(1) (same provisions for actions brought by a state).

¹⁶ See 47 U.S.C. § 227(b)(4)(B) (imposing more stringent penalties for violations of § 227(b) committed “with the intent to cause such violation”)

¹⁷ See *e.g.*, *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 69-70 (2007) (adopting “objectively unreasonable” standard as test for “willful” violations of the Fair Credit Reporting Act).

¹⁸ *Berman v. Freedom Fin. Network, LLC*, 400 F. Supp. 3d 964, 979-80 (N.D. Cal. September 4, 2019), citing *Alea London Ltd. v. Am. Home Servs., Inc.*, 638 F.3d 768, 776 (11th Cir. 2011); *Soppet v. Enhanced Recovery Co., LLC*, 679 F.3d 637, 641 (7th Cir. 2012); *Universal Underwriters Ins. Co. v. Lou Fusz Auto. Network, Inc.*, 401 F.3d 876, 882 n. 3 (8th Cir. 2005); see also *N. L. v. Credit One Bank, N.A.*, 2020 U.S. App. LEXIS 17434, *14-15 (9th Cir. June 3, 2020).

any intent for liability except when awarding treble damages.”¹⁹ It “makes no exception for senders who mistakenly believe that recipients' permission or invitation existed. The issue of intent, or more accurately, the issues of knowledge and willfulness, however, clearly are material to the question of treble damages.”²⁰

The Commission cannot depart from the plain language of the statute. ‘If the intent of Congress is clear, that is the end of the matter; for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress.’”²¹ Accordingly, Assurance’s requested rule that a telemarketer need only have “a reasonable basis to believe that it has the prior express consent of the called party” should be rejected outright.

B. The Commission has Repeatedly Declined to Adopt Similar Broadly Sweeping Rules

Bound by the statute, the Commission has indeed repeatedly refused to adopt broadly sweeping “good faith” exceptions like the one requested by Assurance here. For instance, in its 2003 Order, the Commission ruled that it would ‘reject proposals to create a good faith exception for inadvertent autodialed or prerecorded calls to wireless numbers and proposals to create implied consent[.]’²² In its 2004 Order, the Commission again refused to adopt a broad good faith exception that would extend to all autodialed or prerecorded telemarketing calls to wireless numbers, noting that it had already “considered and declined to adopt a similar proposal in the

¹⁹ *Alea London Ltd.*, 638 F.3d at 776

²⁰ *Universal Underwriters Ins. Co.*, 401 F.3d at 882 n. 3.

²¹ *National Credit Union Admin. v. First Nat. Bank & Trust Co.*, 522 U.S. 479, 499–500 (1998)(quoting, *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 842–843 (1984)).

²² *In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 18 FCC Rcd 14014, at ¶ 172 (2003) (2003 TCPA Order).

2003 TCPA Order.”²³

In its 2015 Order, the Commission again rejected proposals for broadly sweeping exemptions based on “good faith errors.”²⁴ In doing so, it “clarif[ied] that *the caller's intent does not bear on liability*” and “ma[d]e clear that such calls are exactly the types that the TCPA is designed to stop.”²⁵

Contrary to Assurance’s contentions, the Commission has never ruled that “prior express consent” means a “reasonable belief of prior express consent.” Although the Commission has considered a caller’s “reasonable reliance” on consent as a basis for creating limited safe harbors for calls to reassigned and ported telephone numbers, courts have repeatedly held that those orders “did not sanction an affirmative defense based upon the reasonableness of the caller's belief in consent.”²⁶ To be sure, “if a caller's intent could defeat liability, the safe harbors would be unnecessary.”²⁷ Thus, the Commission has never, and indeed cannot consistent with the statute, approve a broad rule injecting an intent test into the determination of “prior express consent.”²⁸

²³ *In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 19 FCC Rcd 19215, 19219-20, ¶ 11 (August 25, 2004) (“2004 Order”).

²⁴ *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 30 FCC Rcd 7961, 7999, ¶ 71 (June 18, 2015) (“2015 Order”).

²⁵ *Id.* at 8003-04, ¶ 80 (emphasis added).

²⁶ *Rawlins v. Stoneberry & Mason Cos.*, 2016 U.S. Dist. LEXIS 184937, *14-15 (N.D. N.Y. September 1, 2016); *see also Jiminez v. Credit One Bank, N.A.*, 377 F. Supp. 3d 324, 335 (S.D.N.Y. 2019) (“the Court declines Defendants’ invitation to recognize a reasonable reliance exception or defense that is inconsistent with the plain language of the statute”); *Perez v. Rash Curtis & Assocs.*, 2019 U.S. Dist. LEXIS 58639, at *13 (N.D. Cal. Apr. 4, 2019) (“defendant may not assert that it acted in good faith in calling Perez and therefore is not liable under the TCPA”);

²⁷ *N. L.*, 2020 U.S. App. LEXIS 17434 at *15

²⁸ Contrary to Assurance’s contentions, *ACA International et al. v. F.C.C.*, 885 F.3d 687 (D.C. Cir. 2018) does not hold otherwise. As the Commission has already found, the court in *ACA International* merely

C. A “Reasonable Basis to Believe” Rule Would Harm Consumers and Create Confusion

The Commission should also reject the proposed “reasonable basis to believe” rule because it will harm consumers and create confusion for callers. As it stands, the statute imposes a bright line rule on telemarketers who want to use prerecorded messages - either obtain “prior express consent” or violate the statute. The proposed rule, however, would fail to describe what exactly is prohibited by law.

Consider the following scenarios. If a home security company pays a data broker to provide it with a list of consumers who have consented to receive telemarketing calls from home security companies, and that list comes with a guarantee by the data broker that the consumers in the list had actually consented, does the telemarketer have a reasonable basis to believe that it has prior express consent to call all the consumers in the list? Many telemarketers would certainly hope that would be enough to satisfy their obligations, but that can’t be enough, right? What if the telemarketer researched the data broker’s reputation and couldn’t find any complaints about the integrity of its data? Is it reasonable now? What if the data set purported to show the specific website URL at which each consumer supposedly provided their contact information and agreed to receive calls? Does the telemarketer have an obligation to review every single one of those URL’s to determine if the consent disclosure is actually compliant with this Commission’s rules? What if it reviewed only a quarter of them? What if the data set didn’t contain any names or addresses, or instead contained a significant number of obviously fake names or addresses, like Mickey Mouse at 123 Main Street, The North Pole? Would the telemarketer’s reliance on the data set be unreasonable in that case? What if the data set showed

“favorably noted” the Commission’s consideration of “reasonable reliance” *as a reason for “establishing a reassigned numbers database and the Commission’s consideration to adopt a safe harbor for callers that check the database.”* 2018 Order, 33 FCC Rcd at 12045, ¶ 58 (emphasis added). The court endorsed no re-interpretation of prior express consent.

that some of the consumer data was actually uploaded to those website URLs by TOR Exit Routers? Would that telemarketer be able to reasonably rely on any of the data in the data set? What if only 2% of the data was uploaded by TOR Exit Routers?

Nobody knows how a court, or this Commission, would answer these questions. The requested rule would therefore leave telemarketers in the dark as to how to comply with the statute. Moreover, a finding that a telemarketer in any one of these scenarios had a reasonable basis to believe it had consent would leave the consumers identified in the data set without any recourse under the TCPA if, in fact, their data had been uploaded without their knowledge, as Mr. Shelton's data was in this case. The Commission should not adopt a rule that will leave consumers without recourse under the TCPA when their data has been stolen or fraudulently supplied to telemarketers over the internet. This is not far-fetched scenario. The lead generation and affiliate marketing industries are rife with fraud.

1. Fraud is Rampant in the Telemarketing Lead Generation Industry

Why are there so many products on sale to telemarketers that are designed identify and block fraudulent lead data?²⁹ Assurance would apparently have the Commission believe it is because bogeymen “serial TCPA litigants” are out there surreptitiously uploading their data in the hopes that they will be called and can then file a lawsuit.³⁰ This is a ridiculous fantasy. Lead fraud is not caused by TCPA litigants, it is caused by a telemarketing lead generation industry run amok. Just look at how the sellers of these products describe the problem:

²⁹ See e.g. IPQualityScore, <https://www.ipqualityscore.com/features/prevent-affiliate-ad-fraud>; e-Hawk, <https://ehawk.net/>; Fraudlogix, <https://www.fraudlogix.com/solutions/affiliate/>; Nura, <https://www.anura.io/>; Partnership Cloud, <https://impact.com/protect-monitor/>.

³⁰ Assurance claims, without any evidence whatsoever, that it “is the victim of a targeted assault—i.e., someone fraudulently supplied accurate contact information for a TCPA litigant onto its website with the apparent intention of providing Mr. Shelton with ammunition to sue Assurance.” Petition, at p. 7. This contention is false and entirely unsupported.

“Dishonest affiliate marketers are able to send traffic that’s anything but profitable your way. You’ll see an increase in site traffic and an influx of leads, but your sales may not improve at all. Why? Because affiliate ad fraud sends traffic from bots, malware, and automated scripts – instead of traffic coming from a real person – to your site. To add insult to injury, you, the owner/advertiser will unknowingly end up compensating the affiliate fraudsters. Often, by the time the fraud is caught, you may be left dealing with a ton of useless leads, lost payouts and a lot of frustration.”³¹

“Pay for leads, not dead-ends

Fraud especially targets lead-generation campaigns, collecting high payments for stolen or recycled info. Gain real-time insights into suspicious traffic sources to quickly identify high-risk partners. Block payments for illegitimate lead and conversion events.”³²

“Many people, from bloggers to influencers, partner with affiliate programs as a way to earn some cash. Using trackable URLs, affiliates direct online traffic to certain websites with the goal of converting visitors into leads. In exchange for securing new leads, companies pay their affiliates a commission for each lead generated. But not all affiliates abide by the rules. Dishonest ones sometimes use bots to crawl the web and scrape consumer information from other sites. The bots then drive traffic through an affiliate link and subsequently fill out lead generation forms with stolen or fraudulent consumer information.”³³

These products exist because fraud is rampant in the online marketing space. The Wall Street Journal reported on the problem in 2018, after a study by Adobe found that about 28% of web traffic came from bots.³⁴ The Commission need look no further than Assurance’s own

³¹ <https://www.fraudlogix.com/affiliate-blog/how-to-safeguard-your-affiliate-campaigns-and-weed-out-ip-addresses-associated-with-ad-fraud/>

³² <https://impact.com/protect-monitor/>.

³³ <https://blog.anura.io/how-lead-fraud-affects-brands-and-consumers;>

³⁴ FRAUDULENT WEB TRAFFIC CONTINUES TO PLAGUE ADVERTISERS, OTHER BUSINESSES, <https://www.wsj.com/articles/fraudulent-web-traffic-continues-to-plague-advertisers-other-businesses-152234801>

website to see why this occurs.

2. Website's Like Assurance's Incentive Lead Generation Fraud

Assurance's website provides a perfect example of why lead generation fraud is so common. The website contains a lead form and consent disclosure that purports to provide prior express consent for hundreds of distinct entities to call whatever telephone numbers are entered on the form:

“By clicking 'View My Quote', I expressly consent by electronic signature to receive marketing communication, including via calls using an automatic telephone dialing system and artificial or pre-recorded messages, emails, and text messages (SMS), from insurance companies or their agents, the owner of this website and its agents, representatives and affiliates, and partner companies to the phone number provided (including any wireless numbers).”³⁵

By its terms, this disclosure would authorize not just Assurance, but literally every insurance company and insurance agent in existence, and almost two hundred distinct “partner companies” to robocall the number provided. When one clicks the “partner companies” link, one sees the following list:³⁶

TCPA Partner Companies

- 1st Century
- Accuquote
- AIG Direct
- AIS
- All Web Leads
- Alliance
- Allstate
- Agentra Healthcare
- Alieria Healthcare
- Angelic Marketing Group
- Alpine Digital Group, Inc.

³⁵ Petition, at p. 3.

³⁶ <https://www.assurance.com/tcpa-partner-companies>

- American Adventure Insurance
- Americare
- Ameriquote
- Answer Financial
- Apollo Interactive
- Art Institute
- Avendia
- Avenge Digital
- Black Optek
- BRXTN Digital Media
- Bantam Connect
- Bayside
- Cege Media
- Choice Direct
- ClearLink
- Click 2 Call Network
- CompareInsuranceQuotes
- Connect Insurance Brands
- Contactability
- Coverage One
- CS Marketing
- Debt.com
- Direct General
- Discount Insurance Quotes
- EasyMedicare.com, an affiliate of e-TeleQuote Insurance, Inc
- Efinancial
- EPIQ
- Esurance
- Excel Impact
- FirstQuoteHealth.com
- Florida Blue
- Fortegra
- Freeway Insurance Services
- Get Seen Media
- Globe Life
- GoHealthInsurance
- Goji
- goMedigap
- Guidetoinsure
- Hannigan Insurance
- Health Benefit Center
- Health Benefits One
- Health Choice One
- HealtheDeals

- Health Insurance Innovations
- Health Insurance Services
- Health IQ
- Health Plans of America
- Health Solutions One
- HealthCare, Inc.
- HealthMarkets
- HealthPlanOne
- Home Insurance King
- Ideal Concepts
- Inside Response
- InsuraMatch
- Insurance Care Direct
- Insurance Quotes Now
- Insurance Services
- IPA Direct
- iWebQuotes
- Kanopy Insurance
- Kelly Klee
- Leadnomics
- Liberty Mutual
- Lighthouse
- MassNexus
- Mercury
- Moss
- Mutual of Omaha
- National General
- Nationwide
- NetQuote
- NextGen Leads, LLC
- Nexus Enterprise Solutions
- Outlook Advisors
- Pay Per Call Market
- Pay Per Call Transfers
- PEMCO
- PFP
- Ping Leads
- Platform Advertising
- Plymouth Rock
- Precursor Media
- Progressive
- Quote Engine
- QuoteWizard
- Rank Media Agency

- RevPoint
- Selective Healthcare
- SelectMyPolicy.com
- SelectQuote
- SolidQuote, LLC
- State Farm
- The Insurance Center
- The Lead Company
- The Zebra
- Tranzact
- Travelers
- Underground Elephant
- United Medicare Advisors
- Velapoint
- Vital One Health
- ZQ Auto Insurance
- Allied Insurance Partners
- easyMedicare.com, an affiliate of e-TeleQuote Insurance, Inc.
- American Income Life Insurance Company Family
- Heritage Life Insurance Company
- Globe Life Insurance Company of New York
- Liberty National Life Insurance Company
- National Income Life Insurance Company
- United American Insurance Company
- Vantis Life
- Prudential
- Smart Health Options, LLC
- American Insurance Company
- Open Market Quotes
- Senior Market Quotes
- Smart Match Insurance Solutions
- Spring Health Plans
- Spring Insurance Solutions
- Tiburon Insurance
- TrueChoice Insurance Services
- Senior Life
- EverQuote, Inc.
- Quantum3media
- Q3MInsuranceSolutions
- Themedicareassistant.com
- Finalexpenseassistant.com
- Healthcareassistant.com
- Benefit Advisors
- Support First

- Legacy Insurance Solutions
- Health Center Marketing
- Inboxed LLC.
- The-Solar-Project.com.
- Clean Energy Concepts
- Green Home Advantage
- Bright Home Energy
- S.B. Fintech Ltd
- Quotehound
- Commercial Insurance Center
- United Insurance Group Agency, Inc.
- Quote Velocity
- Purple Dog Marketing LLC
- Alphatech Resource Holdings s.r.o
- Policy Scout
- PolicyScout
- Disability Advisor
- National Disability
- Citizens Disability
- Premier Disability
- Heard and Smith
- Advocator Group
- STRINGBIT inc.
- Innovation Direct Group
- Presidio Interactive
- Connect Plus
- Insurance Solutions LLC
- Innovate Financial Group
- Blue Summit
- TrustedConsumer
- Mercury Insurance
- Palisades Media Group
- American Insurance Organization, LLC
- Blue Nile

The list identifies data brokers, online marketing companies, debt relief organizations, jewelers, solar energy companies, insurance companies, and who knows what else. It is nearly impossible to tell who exactly many of these entities are. What is “Pay Per Call Transfers”? What is “Moss”? Who knows? And who knows how many affiliate marketers or other lead generators these entities have hired to generate leads for them to call? The only thing that is

clear is that Assurance itself, and every single one of its “TCPA partner companies,” and every single affiliate marketer or lead generator that works for them has a financial incentive to drive consumer data into the web form on Assurance’s website. Affiliates can earn commission by generating leads, the partner companies can call the leads, and Assurance itself can sell the data. Lead generation websites like these are all too common and create markets for fraudulent “consent data.”³⁷

III. THE COMMISSION SHOULD NOT CREATE A SAFE HARBOR FOR “CONSENT DATA”

Assurance asks the Commission to place the burden of lead generation fraud onto consumers. It asks that, in addition to re-defining “prior express consent,” the Commission should rule specifically that telemarketers can rely on data uploaded into lead generation forms “until such time as the called party claims to the caller that he or she did not provide the consent.”³⁸ Such a rule would turn the TCPA on its head.

The TCPA does not require consumers to *opt-out* of robocalls, it requires the opposite - an *opt-in* via “prior express consent.”³⁹ That is why this Commission rejected a similar rule that was proposed to address reassigned numbers, in which callers would be allowed call until they “obtain actual knowledge of reassignment.”⁴⁰ The Commission held that such a rule would “effectively require consumers to opt out of such calls when the TCPA clearly requires the

³⁷ See e.g., <https://searchmynewjob.com/partners>; <https://join.super-samples.com/marketing-partners/>; <https://theultimaterenttoownhomeprogram.com/realrenttoownhomes/10777/002>; <http://www.dlvrd.marketing/partners.php>

³⁸ Petition, at p. 13.

³⁹ 47 U.S.C. § 227(b)(1)

⁴⁰ 2015 Order, 30 FCC Rcd, at 8003-04, ¶ 80.

opposite--that consumers opt in before they can be contacted.”⁴¹ The Commission went on to “reiterate that the TCPA places no affirmative obligation on a called party to opt out of calls to which he or she never consented; the TCPA places responsibility on the caller alone to ensure that he or she has valid consent for each call made using an autodialer, artificial voice, or prerecorded voice.”⁴²

Although the Commission has adopted precise and strictly limited safe harbors when new technologies have made compliance with the statute impossible (*i.e.*, reassigned and ported telephone numbers),⁴³ Assurance is not asking for a limited safe harbor here. Instead, it asks the commission to give telemarketers generalized and sweeping permission to call lead generation data until the called party tells them that, in fact, they do not consent.

Moreover, the requested safe harbor is untied to any specific technological changes, much less any that have made compliance with the TCPA impossible. Internet lead generation fraud is certainly a problem, but it is a problem *created by the telemarketing industry*, which has incentivized fraudulent lead generation via affiliate marketing programs and websites, like Assurance’s, that purport to provide TCPA consent for literally hundreds of distinct and disparate entities that want to robocall consumers and are willing to pay for “consent data.” Telemarketers do not *need* to use data generated by third parties, nor do they need to rely on data entered into online lead generation forms. Robocallers who seek to rely on such data should do so at their own risk. Consumers should not bear the burden of a problem that the robocallers themselves have created and exacerbated by accepting fraudulent data from obviously fraudulent

⁴¹ *Ibid.*

⁴² *Id.* at 8004, ¶ 81.

⁴³ *2004 Order*, 19 FCC Rcd at 19218, ¶ 9; *2018 Order*, 33 FCC Rcd at 12044-45, ¶ 58.

sources, as Assurance did here.

There are, in any event, numerous products on the market⁴⁴ that allow telemarketers to identify suspicious and fraudulent leads, such as those coming from TOR Exit Routers like the one that uploaded Mr. Shelton's personal data to the Assurance site.⁴⁵ Telemarketers can use these, and other measures, to ensure that they are not accepting fraudulent leads. Or, like the rest of us, they can place calls that don't use prerecorded messages. They do not face an impossible situation and the Commission should decline to give telemarketers seeking to rely on such data a free pass.

Consider the effect that the proposed safe harbor would have on consumers, like Mr. Shelton, whose personal data is fraudulently uploaded onto lead generation websites like Assurance's. These websites purport to provide consent for hundreds of distinct telemarketers to call the phone numbers uploaded to the site. The users of those phone numbers would now have the obligation to inform literally hundreds of distinct entities that they do not in fact consent to be called before they could ever assert their rights under the TCPA. That is entirely unreasonable.

IV. THE COMMISSION CANNOT AND SHOULD NOT EXEMPT "SHORT, INTRODUCTORY PRERECORDED MESSAGES" FROM THE TCPA

Assurance also asks the commission to declare the TCPA does not apply to calls that use

⁴⁴ See e.g., IPQualityScore, <https://www.ipqualityscore.com/features/prevent-affiliate-ad-fraud>; e-Hawk, <https://ehawk.net/>; Fraudlogix, <https://www.fraudlogix.com/solutions/affiliate/>; Nura, <https://www.anura.io/>; Partnership Cloud, <https://impact.com/protect-monitor/>; HOW TO BLOCK TOR IN YOUR BUSINESS - BLOCKING MALWARE, DARKNET USE AND ROGUE NODES, <https://www.computerworld.com/article/3427057/tor-and-the-enterprise-2016---risks-of-tor-use-inside-a-network---how-to-block-tor-in-your-business-.html>;

⁴⁵ Assurance claims that it uses a product called "TrustedForm", to "verify the origin and authenticity of Internet leads," but that product appears to simply create a record of the data transmission, rather than actually block any fraudulent or suspicious data. See <https://activeprospect.com/trustedform/>

only “a short, introductory prerecorded message” before a human being begins speaking to the called party. Again, Assurance asks the commission to rewrite the TCPA.

To be sure, adopting such a rule is virtually guaranteed to result in an explosion of robocalls. Consumers could expect an unending barrage of calls like the following:

“Are you interested in hearing about an exciting [vacation opportunity]? If so, stay on the line to talk with Amy.”

Indeed, Assurance is filing its petition because it uses exactly this type of prerecorded message in its calls.⁴⁶ This is precisely what the TCPA was originally enacted to address – the use of prerecorded messages to convey telemarketing messages and weed out anybody who hangs up because they don’t want to talk to telemarketers.

Assurance claims that the TCPA only applies to calls that are “entirely prerecorded and “fully automated,”⁴⁷ but it does not, and indeed cannot, cite *any language in the statute* that supports its interpretation. The plain language of the statute requires prior express consent to make any call to a cell phone “*using . . . an artificial or prerecorded voice.*”⁴⁸ Similarly, the statute requires prior express consent to initiate any telemarketing call to a residential line “using an artificial or prerecorded voice to deliver a message.”⁴⁹ The Commission does not have the authority to re-write the statute by adding “except when the prerecorded voice is used only in a short, introductory message.”

Not only do the statutory provisions at issue plainly cover the mere *use* of a prerecorded

⁴⁶ Petition, at p. 5 (“I am here to help you with your insurance needs”)

⁴⁷ Petition, at p. 10.

⁴⁸ 47 U.S.C. § 227(b)(1)(A).

⁴⁹ 47 U.S.C. § 227(b)(2). It is unclear if Assurance is even asking the commission to make a declaratory ruling concerning this provision, as Assurance has styled its petition as a request for a “declaratory ruling regarding the application of 47 U.S.C. § 227(b)(1) of the Telephone Consumer Protection Act.” Petition, at Cover.

voice, there is no “automation” requirement for prerecorded voice calls whatsoever. Otherwise, there would be no reason for Congress to *separately* regulate the use of automatic telephone dialing systems.⁵⁰

And beyond the plain language of the statute, the legislative history confirms that Congress intended to regulate prerecorded messages played on an “otherwise live call”:

“when a consumer answers the phone, a ‘live’ person can ask the consumer if he or she consents to listening to a recorded or computerized message. If the consumer indicates express consent, the ‘live’ caller may switch to a record-ed or computerized message. The Committee does not believe that this consent requirement will be an inordinate regulatory burden on the telemarketer.”⁵¹

Thus, Assurance is asking the Commission to both disregard the plain language of the statute and the legislative will.

Assurance also claims that that this Commission has itself “consistently suggested the phrase ‘using an artificial or prerecorded voice to deliver a message’ refers to calls that are entirely prerecorded and fully automated for more than 25 years.”⁵² Yet not a single one of the FCC documents that Assurance cites actually says that, or anything like it. Rather than imposing an “entirely prerecorded” or “fully automated” requirement that does not exist in the statute, this commission has instead repeatedly confirmed that it is simply unlawful to use a prerecorded voice to deliver telemarketing messages. *See, e.g. Citation to Direct Link, Inc., d.b.a. Live Link Technologies*, 21 FCC Rcd 3395 (March 31 2006) (“it is generally unlawful to use an artificial or prerecorded voice to deliver an advertisement or telephone solicitation to a residential telephone

⁵⁰ See 47 U.S.C. § 227(b)(1)(A) (regulating calls using any “automatic telephone dialing system or an artificial or prerecorded voice”) (emphasis added).

⁵¹ Senate Committee Report, S. Rep. 102-178-1991 pg. 8; *see also* comments of Senator Hollings upon introduction and passage of S. 1462 (the TCPA) on November 7, 1991 (Senate Record 137-Cong. Rec. 16204, 1991) (“Such consent also could be obtained by a live person who simply asks the called party whether he or she agrees to listen to a recorded message.”)

⁵² Petition, at p. 10.

line . . .’).’ *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 27 FCC Rcd. 1830, 1838, ¶ 20 (February 15, 2012) (“we require prior express written consent for all telephone calls using an automatic telephone dialing system or a prerecorded voice to deliver a telemarketing message to wireless numbers and residential lines.”); *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 30 FCC Rcd 7961, 7967 (July 10, 2015) (“The TCPA and the Commission's implementing rules prohibit: (1) making telemarketing calls using an artificial or prerecorded voice to residential telephones without prior express consent and (2) making any non-emergency call using an automatic telephone dialing system ("autodialer") or an artificial or prerecorded voice to a wireless telephone number without prior express consent”). Assurance’s calls do exactly that.

Assurance also claims that this commission’s regulation at 47 C.F.R. § 64.1200(b)(2), which requires the disclosure of the caller’s telephone number in “all artificial or prerecorded voice telephone messages” only applies to “fully automated robocalls.” The scope of that rule, however, is not at issue here, and indeed the language differs substantially from § 227(b). Compare “prerecorded voice *telephone messages*” to “*using an artificial or prerecorded voice.*” So even it were true that this Commission’s disclosure requirement rule in 47 C.F.R. § 64.1200(b)(2) only applied to “fully automated robocalls,” whatever that means, that would say nothing about whether Congress’s prohibition in section 227(b) against *using an artificial or prerecorded voice* without the prior express consent of the called party had the same limitation.

Next, Assurance claims that an appellate decision from 1995 (*Moser v. F.C.C.*, 46 F.3d 970 (9th 1995)) held that prerecorded messages in “otherwise live” calls are not regulated by the TCPA. *Moser* made no such holding. Indeed, such calls were simply not at issue in that case.

In *Moser*, a telemarketing association sued the FCC arguing that the TCPA's prohibitions against prerecorded telemarketing calls to residential lines in 47 U.S.C. § 227(b)(1)(B) violated the First Amendment of the United States Constitution. *Id.* at 973. The Court rejected that argument because § 227(b)(1)(B)'s restrictions on calls to residential lines "leave open many alternative channels of communication." *Id.* at 975. It suggested that telemarketers could, for instance, still call residential numbers with "live solicitation calls", "taped messages to which consumers have consented," and "taped messages introduced by live speakers[.]" *Ibid.* Contrary to Assurance's claims, this does not suggest that "short, introductory prerecorded messages in otherwise live calls" are unregulated by the TCPA. Instead, it simply reflects what Congress had already expressed in the legislative history – if a "live" person wants to play a prerecorded telemarketing message over the phone, then "when [the] consumer answers the phone, a 'live' person can ask the consumer if he or she consents to listening to a recorded or computerized message. If the consumer indicates express consent, the 'live' caller may switch to a record-ed or computerized message."⁵³

This Commission should therefore follow the guidance of Federal Trade Commission's 2016 Staff Opinion Letter concerning the application of the FTC's linguistically similar Telemarketing Sales Rule ("TSR") to this type of soundboard technology. In that letter, FTC staff found:

"the plain language of the TSR provision governing prerecorded calls imposes restrictions on "any outbound telephone call that delivers a prerecorded message." It is indisputable that calls made using soundboard technology deliver prerecorded messages. As such, under the plain meaning of the words in the TSR's prerecorded call provision, outbound telemarketing

⁵³ Senate Committee Report, S. Rep. 102-178-1991 pg. 8; *see also* comments of Senator Hollings upon introduction and passage of S. 1462 (the TCPA) on November 7, 1991 (Senate Record 137- Cong. Rec. 16204, 1991) ("Such consent also could be obtained by a live person who simply asks the called party whether he or she agrees to listen to a recorded message.")

calls using soundboard technology are covered because such calls “deliver a prerecorded message.”⁵⁴

This Commission has repeatedly stated that it seeks to harmonize its rules with the FTC’s TSR.⁵⁵ Exempting “short, introductory prerecorded messages” from the TCPA simply because they are played in an “otherwise live call” would not only contravene the plain language of the statute, it would create a conflict between the TCPA and the FTC staff’s guidance on the TSR, leading to uncertainty and incongruity in the regulation of prerecorded voice calls.

V. A RESPONSE TO THE AD HOMINEM ATTACK ON MR. SHELTON

Mr. Shelton rightly filed a lawsuit against Assurance because it violated numerous provisions of the TCPA and continued to send him automated messages even after he asked it to stop.⁵⁶ Not only did Assurance robocall Mr. Shelton’s phone number without his consent, it spoofed its calls to make it appear as if a local telephone number was calling.⁵⁷ Moreover, it accepted obviously fraudulent data from a Tor Exit Router and now claims that it had no reason to question it.

In an effort to deflect from its own misconduct, Assurance engages in ad hominen attack on Mr. Shelton as a “serial” litigant and contends that it was set up just so Mr. Shelton could sue it. This is ridiculous. As shown above, lead generation fraud is widespread and is not caused by TCPA litigants, but instead by the affiliate marketing and telemarketing lead generation industries.

⁵⁴ https://www.ftc.gov/system/files/documents/advisory_opinions/letter-lois-greisman-associate-director-division-marketing-practices-michael-bills/161110staffopsoundboarding.pdf

⁵⁵ *In re Rules and Regulations Implementing the Telephone Consumer Protection Act*, 27 FCC Rcd. 1830, 1831 (February 15, 2012); *In re Joint Petition Filed by Dish Network*, 28 FCC Rcd. 6574, 6588 (May 9, 2013)

⁵⁶ *Shelton v. Lumico et al*, Case 7:19-cv-06494, Doc. 1 (S.D. N.Y. July 12, 2019).

⁵⁷ *Id.*

When Mr. Shelton, the owner of a small business that enforces civil judgments, files lawsuits seeking relief under the TCPA, he essentially acts as a private attorney general. This is exactly what the TCPA was designed to encourage consumers to do. The TCPA and the statutory damages it offers plaintiffs are “specifically designed to appeal to plaintiff’s self-interest and to direct that self-interest toward the public good” with statutory damages operating as rewards, or “bounties,” for catching telemarketers engaged in illegal practices to them.⁵⁸ Thus, “in creating a private right of action under the TCPA, Congress chose to incent private litigants to enforce the law, rather than having government regulators do it. The fact that Mr. Shelton and other litigants respond to the economic incentives that Congress created is not evidence of misconduct.”⁵⁹ Courts across the country have reiterated this point.⁶⁰

Assurance also claims that Mr. Shelton is someone deserving of scrutiny simply because someone filed a lawsuit against him in a retaliatory action after Mr. Shelton successfully sued them in a prior lawsuit. That retaliatory action has not resulted in any finding of wrongdoing by Mr. Shelton, but instead in the Court entering sanctions against the party that brought it.⁶¹

⁵⁸ *Cunningham v. Rapid Response Monitoring Servs.*, 251 F. Supp. 3d 1187, 1195 (M.D. Tenn. 2017).

⁵⁹ *Shelton v. FCS Capital LLC*, Case No. 2:18-cv-03723-JDW, 2020 U.S. Dist. LEXIS 105730 (E.D. Pa. June 17, 2020)

⁶⁰ See *Charvat v. Echostar Satellite, LLC*, 630 F.3d 459, 461 (6th Cir. 2010) (“Phillip Charvat has not been shy in taking on the role of a private attorney general under the [TCPA].”); *Universal Underwriters Ins. Co. v. Lou Fusz Automotive Network, Inc.*, 401 F.3d 876, 881 (8th Cir. 2005) (private right of action under TCPA demonstrates Congressional intent to incentivize aggrieved parties to act as “private attorneys general”); *Mey v. Venture Data, LLC*, 245 F. Supp. 3d 771, 783 (N.D.W. Va. 2017) (denying a motion for summary judgment in a TCPA case holding, “It is true that the plaintiff has brought a number of TCPA cases. It is further true that she has telephone answering and recording equipment[, but] [t]his does not deprive the plaintiff of standing any more than the purchase of a burglar alarm would indicate that the homeowner wanted her house to be broken into.... While [defendant] is understandably frustrated by Ms. Mey’s efficacy, she is doing exactly what Congress intended—enforcing the law.”)

⁶¹ No. 2:20-cv-163 (March 27, 2020)

The Commission should accordingly disregard the ad hominen attacks and not penalize consumers who do exactly what the TCPA was created for them to do – sue to enforce the law.

Respectfully submitted,

By: /s/ Timothy J. Sostrin
Timothy J. Sostrin

Timothy J. Sostrin
Keith J. Keogh
Keogh Law LTD
55 W Monroe St, Ste. 3390
Chicago, IL 60603
(312) 726-1092
tsostrin@keoghlaw.com
keith@keoghlaw.com

and

Anthony I. Paronich
Paronich Law, P.C.
350 Lincoln Street, Ste. 2400
Hingham, MA 02043
(508) 221-1510
anthony@paronichlaw.com

Attorneys for James Shelton